CHAPTER 2

NETWORKING STANDARDS AND THE OSI MODEL

After reading this chapter and completing the exercises, you will be able to:

- Identify organizations that set standards for networking
- Explain the layers of the OSI Model
- Describe specific networking services within each layer of the OSI Model
- Explain how two systems communicate through the OSI Model
- Discuss the structure and purpose of data frames
- Describe the two types of addressing contained in the OSI Model

ON THE JOB

When I first heard about the OSI Model, I had already been working as a networking technician for a few months. I thought I knew all about NICs and cabling, but I didn't know the OSI layer to which they belonged. When someone tried to teach me about the OSI Model, I thought it was baloney. The more I learned, however, the more I realized I didn't understand. For example, once a colleague and I tried to figure out why a networked printer wasn't printing. He insisted that it was a "Layer 3 problem." I didn't know what he meant, so I couldn't agree or disagree. From the symptoms, I thought that the printer was probably experiencing an addressing conflict with another device. The printer worked for a while, but after we restarted it, the network didn't recognize it. I didn't know whether this error was a Layer 3 problem; not wanting to sound foolish, I didn't say anything at all. Luckily, an addressing conflict is exactly what my colleague meant by a "Layer 3 problem," and he quickly fixed the problem.

You can be sure that I quietly figured out what "Layer 3" meant shortly after that incident. Since then, I've noticed that an increasing number of people refer to networking hardware, applications, or problems by the OSI Model layer involved. For instance, one networking hardware manufacturer's slogan is "Providing solutions for Layers 1–3." The company doesn't even have to mention the OSI Model, because anyone involved in networking understands the message.

These days we take for granted that servers and clients from different hardware manufacturers, such as Compaq, IBM, Dell, and Hewlett-Packard, will work together. Before the OSI Model, no standard existed, which meant that computing professionals could not assume any kind of compatibility between different manufacturers' hardware and software. Believe it or not, the OSI Model has made our lives easier.

Andy Zimmerman
MedTech Data Systems

When trying to grasp a new theoretical concept, it often helps to form a picture of that concept in your mind. In the field of chemistry, for example, even though you can't see a water molecule, you can represent it with a simple drawing of two hydrogen atoms and one oxygen atom. Similarly, in the field of networking, even though you can't see the communication that occurs between two nodes on a network, you can use a model to depict how the communication takes place. The model commonly used to describe network communications is called the Open Systems Interconnection (OSI) Model.

In this chapter, you will learn about the standards organizations that have helped create the various models (such as the OSI Model) used in networking. Next, you'll be introduced to the seven layers of the OSI Model and learn how they interact. You will then take a closer look at what goes on in each layer. Finally, you will learn to apply those details to a practical networking environment. Granted, learning the OSI Model is not the most exciting part of becoming a networking expert. Unless you understand it thoroughly, however, you will never become an expert.

NETWORKING STANDARDS ORGANIZATIONS

Standards are documented agreements containing technical specifications or other precise criteria that stipulate how a particular product or service should be designed or performed. Many different industries use standards to ensure that products, processes, and services suit their purpose. For example, when plastics manufacturers test their products for flexibility, the tests must adhere to strict American National Standards Institute (ANSI) specifications so that the results can be accurately compared with other manufacturers' results. If manufacturers didn't use the same ANSI test, one company might test flexibility by pulling on the plastic, while one might test flexibility by poking it. The flexibility numbers that each manufacturer obtained, even for the same type of plastic, would then be completely different, and consumers could not compare the two products' flexibility.

Because of the wide variety of hardware and software in use today, standards are especially important in the world of networking. Without standards, you could not design a network because one piece of hardware might not work properly with another. Likewise, one software program might not be able to communicate with another. For example, if one manufacturer designed a network cable with a 1-centimeter-wide plug and another company manufactured a wall plate with a 0.8-centimeter-wide opening, you would not be able to insert the cable into the wall plate.

Because the computer industry grew so quickly out of several technical traditions, many different organizations evolved to oversee its standards. In some cases, a few organizations are responsible for a single aspect of networking. For example, both ANSI and ITU are involved in setting standards for Integrated Services Digital Network (ISDN) communications. While ANSI prescribes the kind of hardware that the consumer needs to accept an ISDN connection, ITU prescribes how the ISDN link will ensure that data arrive in the correct sequence, among other things. A complete list of the standards that regulate computers and networking would fill an encyclopedia. At a minimum, you should be familiar with the handful of significant groups that set the standards referenced by manuals, articles, and books. These groups are responsible for establishing the future of networking.

ANSI

ANSI (American National Standards Institute) is an organization composed of more than 1000 representatives from industry and government who together determine standards for the electronics industry in addition to other fields, such as chemical and nuclear engineering, health and safety, and construction. ANSI also represents the United States in setting international standards. This organization does not dictate that manufacturers comply with its standards, but requests them to comply voluntarily. Of course, manufacturers and developers benefit from compliance, because compliance assures potential customers that the systems are reliable and can be integrated with an existing infrastructure. New electronic equipment and methods must undergo rigorous testing to prove they are worthy of ANSI's approval.

An example of an ANSI standard is ANSI T1.240-1998, "Telecommunications—Operations, Administration, Maintenance, and Provisioning (OAM&P)—Generic Network Information Model for Interfaces between Operations Systems and Network Elements." You can purchase ANSI standards documents online from ANSI's Web site (*www.ansi.org*) or find them at a university or public library. You need not read complete ANSI standards to be a competent networking professional, but you should understand the breadth and significance of ANSI's influence.

EIA

EIA (Electronic Industries Alliance) is a trade organization composed of representatives from electronics manufacturing firms across the United States. EIA began as the Radio Manufacturers Association (RMA) in 1924; over time, it evolved to include manufacturers of televisions, semiconductors, computers, and networking devices. This group not only sets standards for its members, but also helps write ANSI standards and lobbies for legislation favorable to the growth of the computer and electronics industry.

EIA is divided into several subgroups: the Telecommunications Industry Association (TIA); the Consumer Electronics Manufacturers Association (CEMA); the Electronic Components, Assemblies, and Materials Association (ECA); the JEDEC (Joint Electron Device Engineering Council); Solid State Technology Association; the Government Division; and the Electronic Information Group (EIG). In addition to lobbying and setting standards, each specialized group sponsors conferences, exhibitions, and forums in its area of interest. You can find out more about EIA from its Web site: *www.eia.org*.

IEEE

The **IEEE (Institute of Electrical and Electronic Engineers),** or "I-triple-E," is an international society composed of engineering professionals. Its goals are to promote development and education in the electrical engineering and computer science fields. To this end, IEEE hosts numerous symposia, conferences, and local chapter meetings and publishes papers designed to educate members on technological advances. It also maintains a

standards board that establishes its own standards for the electronics and computer industry and contributes to the work of other standards-setting bodies, such as ANSI.

IEEE technical papers and standards are highly respected in the networking profession. Among other places, you will find references to IEEE standards in the manuals that accompany network interface cards. Following are just a few examples of IEEE standards: "Information Technology Year 2000 Test Methods," "Virtual Bridged Local Area Networks," and "Software Project Management Plans." Hundreds more are currently in use. You can order these documents online from IEEE's Web site (*www.ieee.org*) or find them in a university or public library.

ISO

ISO (International Organization for Standardization) is a collection of standards organizations representing 130 countries; its headquarters is located in Geneva, Switzerland. ISO's goal is to establish international technological standards to facilitate global exchange of information and barrier-free trade. Given the organization's full name, you might assume it should be called "IOS," but "ISO" is not meant to be an acronym. In fact, "iso" is the Greek word for "equal." Using this term conveys the organization's dedication to standards.

ISO's authority is not limited to the information-processing and communications industry, but also applies to the fields of textiles, packaging, distribution of goods, energy production and utilization, shipbuilding, and banking and financial services. The universal agreements on screw threads, bank cards, and even the names for currencies are all products of ISO's work. In fact, only about 500 of ISO's nearly 12,000 standards apply to computer-related products and functions. International electronics and electrical engineering standards are separately established by the International Electrotechnical Commission (IEC), a similar international standards body. All of ISO's information technology standards are designed in tandem with the IEC. You can find out more about ISO at its Web page: *www.iso.ch*.

ITU

The **ITU (International Telecommunication Union)** is a specialized United Nations agency that regulates international telecommunications, including radio and TV frequencies, satellite and telephony specifications, networking infrastructure, and tariffs applied to global communications. It also provides developing countries with technical expertise and equipment to advance those nations' technological bases.

The ITU was founded in Paris in 1865. It became part of the United Nations in 1947 and relocated to Geneva, Switzerland. Its standards arm contains members from 188 countries and publishes detailed policy and standards documents that can be found on its Web site: *www.itu.int*. Typically, ITU's documents pertain more to global telecommunications issues than to industry technical specifications. Some examples of ITU documents

are "Communications for Rural and Remote Areas," "Telecommunication Support for the Protection of the Environment," and "The International Frequency List."

Note: The ITU used to be called the CCITT, or Consultative Committee on International Telegraph and Telephony. You may still see references to CCITT standards in manuals and texts.

THE OSI MODEL

In the early 1980s, ISO began work on a universal set of specifications that would enable computer platforms across the world to communicate openly. The organization created a helpful model for understanding and developing computer-to-computer communications. This model, called the **Open Systems Interconnection (OSI) Model**, divides networking architecture into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer has its own set of functions and interacts with the layers directly above and below it. At the top, the Application layer interacts with the software you use (such as a word-processing or spreadsheet program). At the bottom of the OSI Model are the networking cables and connectors that carry signals. Generally speaking, every layer in between the top and bottom layers ensures that data are delivered in a readable, error-free, and properly sequenced format.

Note: The combination of a network's building blocks is often described as its "architecture." The use of the term "architecture" in the networking field reflects the fact that, like a building, a network contains many distinct but integrated elements: the cabling, servers, protocols, clients, applications, NICs, and so on. A professional involved in network design is sometimes called a **network architect**.

The OSI Model is a theoretical representation of what happens between two nodes on a network. It does not prescribe the type of hardware or software that should support each layer. Nor does it describe how software programs interact with other software programs or how software programs interact with humans. Everything you will learn about networking can be associated with a layer of this model, however, so you should know not only the names of the layers, but also their functions and the way in which the layers interact. Figure 2-1 depicts the OSI Model and its layers.

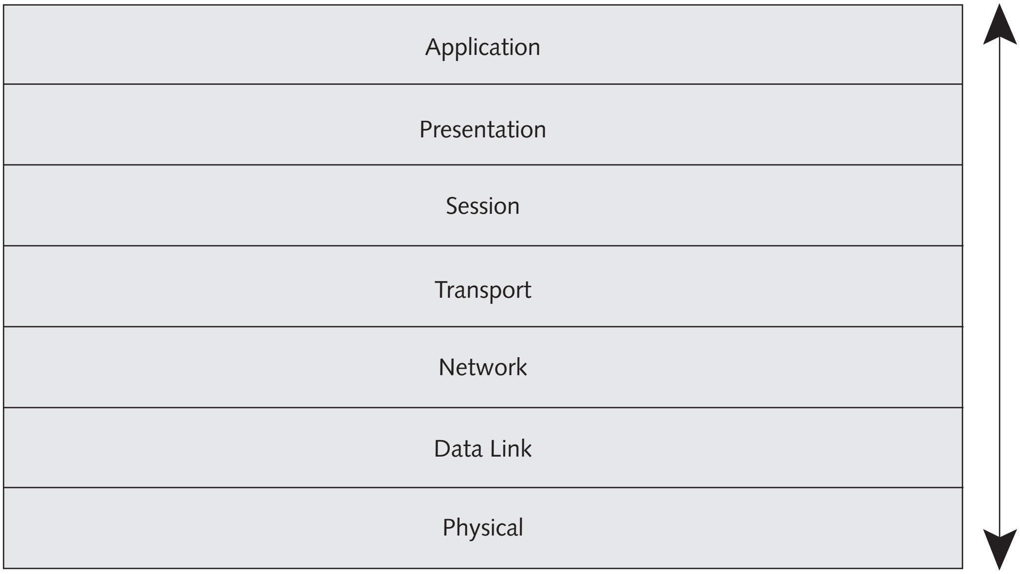

Figure 2-1 The OSI Model

> Tip
>
> Networking professionals typically devise their own mnemonics for remembering the seven layers of the OSI Model. One strategy is to make a sentence using words that begin with the same first letter of each layer, starting with the Physical layer and ending with the Application layer. For example, you might choose to remember the phrase "Phil Donahue Never Televises Sick People Anymore." If the mnemonic phrase you create is quirky or unexpected, you'll probably remember it more easily.

Physical Layer

The **Physical layer** is the lowest, or first, layer of the OSI Model. This layer contains the physical networking medium, such as cabling, connectors, and repeaters. Protocols at the Physical layer generate and detect voltage so as to transmit and receive signals carrying data. When you install a NIC in your desktop PC, you are establishing the foundation that allows the computer to be networked. In other words, you are providing a Physical layer. The Physical layer sets the data transmission rate and monitors data error rates, though it does not provide error correction services. Physical network problems, such as a severed wire, affect the Physical layer. Similarly, if you insert a NIC but fail to seat it deeply enough in the computer's circuit board, your computer will experience network problems at the Physical layer.

The IEEE has set standards for protocols used at the Physical layer. In particular, the IEEE 802 standards specify how data is handled by Ethernet and Token Ring networks (see Chapter 3). The terms "Layer 1 protocols" and "Physical layer protocols" refer to the

standards that dictate how the electrical signals are amplified and transmitted over the wire. Devices that operate at the Physical layer include repeaters and hubs. NICs operate at both the Physical layer and at the Data Link layer (discussed next). You will learn more about Physical layer devices and their operation in Chapters 4 and 6.

Data Link Layer

The second layer of the OSI Model, the **Data Link layer**, controls communications between the Network layer and the Physical layer. Its primary function is to divide data it receives from the Network layer into distinct frames that can then be transmitted by the Physical layer. A **frame** is a structured package for moving data that includes not only the raw data, or "payload," but also the sender's and receiver's network addresses, and error checking and control information. The addresses tell the network where to deliver the frame, whereas the error checking and control information ensure that the frame arrives without any problems.

It may be helpful to envision data frames as trains with many cars. Some of these cars may not be necessary, and the amount of cargo carried by each train will vary, but every train needs an engine and a caboose. Just as different kinds of trains may position their cars in slightly different arrangements, different kinds of frames may arrange their components differently. Figure 2-2 shows a simplified picture of a data frame. Each component of this frame is essential and common to all types of frames. Ethernet and Token Ring frames and their components will be described in detail later in this chapter.

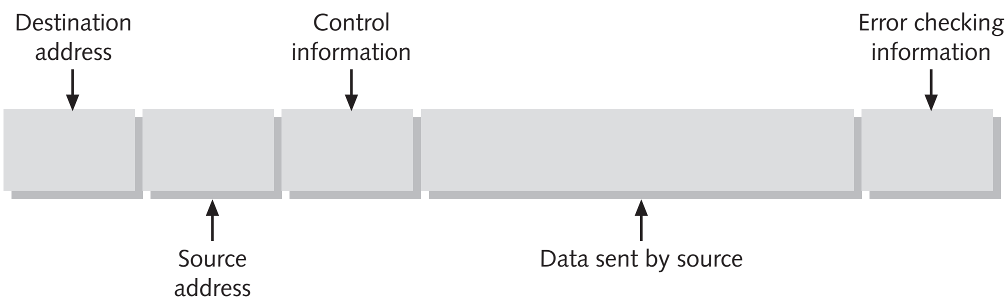

Figure 2-2 A simplified data frame

To fully understand the function of the Data Link layer, pretend for a moment that computers communicate as humans do. You might be in a large classroom full of noisy students and need to ask the teacher a question. Your teacher's name is Ms. Jones. To get your message through, you might say, "Ms. Jones? Can you explain more about the effects of railroads on commerce in the mid-nineteenth century?" In this example, you are the sender (in a busy network) and you have addressed your recipient, Ms. Jones, just as the Data Link layer addresses another computer on the network. In addition, you have formatted your thought as a question, just as the Data Link layer formats data into frames that can be interpreted by receiving computers.

What happens if the room is so noisy that Ms. Jones hears only part of your question? For example, she might receive "on commerce in the late-nineteenth century?" This kind of error can happen in network communications as well (because of electrical interference or wiring problems). The Data Link layer's job is to find out that information has been dropped and ask the first computer to retransmit its message—just as in a classroom setting Ms. Jones might say, "I didn't hear you. Can you repeat the question?" The Data Link layer accomplishes this task through a process called error checking. Later in this chapter, you will learn more about error checking.

In general, the sender's Data Link layer waits for acknowledgment from the receiver that data was received correctly. If the sender does not get this acknowledgment, its Data Link layer gives instruction to retransmit the information. The Data Link layer does not try to figure out what went wrong in the transmission. Similarly, as in a busy classroom, Ms. Jones will probably say, "Pardon me?" rather than, "It sounds as if you might have a question about railroads, and I heard only the last part of it, which dealt with commerce, so I assume you are asking about commerce and railroads; is that correct?" Obviously, the former method is more efficient for both the sender and the receiver.

Another communications mishap that might occur in a noisy classroom or on a busy network is a glut of communication requests. For example, at the end of class, 20 people might ask Ms. Jones 20 different questions at once. Of course, she can't pay attention to all of them simultaneously. She will probably say, "One person at a time, please," then point to one student who asked a question. This situation is analogous to what the Data Link layer does for the Physical layer. One node on a network (a server, for example) may receive multiple requests that include many frames of data each. The Data Link layer controls the flow of this information, allowing the NIC to process data without error.

The Data Link layer functions independently of the type of Physical layer used by the network and its nodes. It also doesn't care whether you are running WordPerfect or Excel or using the Internet. Connectivity devices, such as bridges and switches, work in the Data Link layer, because they decode frames and use the frame information to transmit data to its correct recipient. Ethernet is an example of a Data Link layer technology. Chapters 3 and 6 both discuss elements of the Data Link layer.

Network Layer

The primary function of the **Network layer**, the third layer in the OSI Model, is to translate network addresses into their physical counterparts and decide how to route data from the sender to the receiver. For example, a computer might have a network address of 10.34.99.12 (if it's using the TCP/IP protocol) and a physical address of 0060973E97F3. In the classroom example, this addressing scheme is like saying that "Ms. Jones" and "U.S. citizen with Social Security number 123-45-6789" are the same person. Even though there may be other people named "Ms. Jones" in the United States, only one person has the Social Security number 123-45-6789. Within the confines of your classroom, however, there is only one Ms. Jones, so you can be certain the correct person will respond when you say, "Ms. Jones?"

The Network layer determines the best path from point A on one network to point B on another network by factoring in delivery priorities, network congestion, quality of service, and cost of alternative routes. Because the Network layer handles routing, **routers**—the devices that connect network segments and intelligently direct data—belong in the Network layer. In networking, the term "to **route**" means to direct data based on addressing, patterns of usage, and availability. Chapter 6 explains routers and their functions in detail.

The Network layer protocols also accomplish segmentation and reassembly of packets. **Segmentation** refers to the process of decreasing the size of the data units when moving data from a network segment that can handle larger data units to a network segment that can handle only smaller data units. This process is just like the process of breaking down words into recognizable syllables that a small child uses when learning to read. **Reassembly** is the process of reconstructing the segmented data units. To continue the reading analogy, when a child understands the separate syllables, he can combine them into a word—that is, reassemble the parts into a whole.

Note

The segmentation that takes place in the Network layer of the OSI Model has nothing to do with network segmentation, which was introduced in Chapter 1 and will be described in more detail in Chapter 4. Segmentation in the Network layer refers to a reduction in the size of the data frames, while network segmentation refers to the separation of a network into smaller logical or physical pieces.

Transport Layer

The **Transport layer** is primarily responsible for ensuring that data are transferred from point A to point B (which may or may not be on the same network segment) reliably, in the correct sequence, and without errors. The Transport layer may be considered the most important layer in the OSI Model because without it, data could not be verified or interpreted by their recipients. Transport protocols also handle **flow control**, or the method of gauging the appropriate rate of transmission based on how fast the recipient can accept data.

In addition, Transport layer services break arbitrarily long packets into the maximum size that the type of network in use can handle. For example, Ethernet networks cannot accept packets larger than 1500 bytes. When the sending node's Transport layer services divide its data into smaller pieces, they assign a sequence number to each piece, so that the data can be reassembled in the correct order by the receiving node's Transport layer services. This process is called **sequencing**.

To understand how sequencing works, consider the classroom example again. Suppose you asked the question, "Ms. Jones? How did poor farming techniques contribute to the Dust Bowl?" but that the words arrived at Ms. Jones's ear as "poor farming techniques Ms. Jones? how did to the Dust Bowl? contribute." On a network, the Transport layer would recognize this disorder and rearrange the data pieces so that they make sense. In

addition, the Transport layer sends an **acknowledgment (ACK)** to notify the sender that data were received correctly. If the data contained errors, the Transport layer would request that the sender retransmit the data. Also, if the data weren't acknowledged within a given time period, the sender's Transport layer would consider the data lost and retransmit them.

One service that works in the Transport layer is TCP (Transmission Control Protocol) of the TCP/IP protocol suite. Another Transport layer service is SPX (Sequence Packet Exchange) of the IPX/SPX protocol suite. You will learn more about these and other Transport layer services in Chapter 3.

Session Layer

The **Session layer** is responsible for establishing and maintaining communication between two nodes on the network. The term **session** refers to a connection for data exchange between two parties; it is most often used in the context of terminal and mainframe communications, in which the **terminal** is a device with little (if any) of its own processing or disk capacity that depends on a host to supply it with applications and data processing services. Among the Session layer's functions are establishing and keeping alive the communications link for the duration of the session, synchronizing the dialog between the two nodes, determining whether communications have been cut off, and, if so, figuring out where to restart transmission. Often you will hear the Session layer called the "traffic cop" of network communications. When you dial your Internet service provider (ISP) to connect to the Internet, the Session layer services at your ISP's server, and on your PC client, negotiate the connection. If your phone line is accidentally pulled out of the wall jack, the Session layer on your end will detect the loss of a connection and initiate attempts to reconnect.

The Session layer also sets the terms of communication by deciding which node will communicate first and how long a node can communicate. In this sense, the Session layer acts as a judge in a debate competition. For example, if you were a member of a debate team and had two minutes to state your opening argument, the judge might signal you after one and a half minutes that you have only 30 seconds remaining. If you tried to interrupt a member of the opposing debate team, he would tell you to wait your turn. Finally, the Session layer monitors the identification of session participants, ensuring that only the authorized nodes can access the session.

Presentation Layer

The **Presentation layer** serves as a translator between the application and the network. At the Presentation layer, data become formatted in a schema that the network can understand; this format varies with the type of network used. The Presentation layer also manages data encryption and decryption, such as the scrambling of system passwords. For example, if you look up your bank account status on the Internet, you are using a secure connection, and your account data will be encrypted before they are transmitted.

On your end of the network, the Presentation layer will decrypt the data as they are received. In addition, Presentation layer protocols code and decode graphics and file format information.

Application Layer

The top, or seventh, layer of the OSI Model is the Application layer. The **Application layer** provides interfaces to the software that enable programs to use network services. The term "Application layer" does not refer to a particular software application, such as Microsoft Word, running on the network. Instead, some of the services provided by the Application layer include file transfer, file management, and message handling for electronic mail. For example, if you are running Microsoft Word on a network and choose to open a file, your request for that data is transferred from Microsoft Word to the network by the Application layer.

The part of Microsoft Word that handles this request is its application program interface (API). An **application program interface** is a routine (a set of instructions) that allows a program to interact with the operating system. APIs belong to the Application layer of the OSI Model. Programmers use APIs to establish links between their code and the operating system. An example of an API used in a network environment is **Microsoft Message Queueing (MSMQ)**. MSMQ stores messages sent between nodes in queues and then forwards them to their destinations based on when the link to the recipient becomes available. As a result, programs can run independently of whether the data's destination is connected to the network when the messages are sent.

Applying the OSI Model

Now that you have been introduced to the seven layers of the OSI Model, you can take a closer look at exactly how the layers interact. For reference, Table 2-1 summarizes the functions of the seven OSI Model layers.

Table 2-1 Functions of the OSI layers

OSI Layer	Function
Application	Transfers information from program to program
Presentation	Handles text formatting and displays code conversion
Session	Establishes, maintains, and coordinates communication
Transport	Ensures accurate delivery of data
Network	Determines transport routes and handles the transfer of messages
Data Link	Codes, addresses, and transmits information
Physical	Manages hardware connections

Communication Between Two Systems

An exemplary process to trace through the OSI Model layers is the retrieval of a message file from the server. Once you log in to the network and start your mail program, you can choose to pick up your mail. At that point, the Application layer recognizes your choice and formulates a request for data from a remote node (in this case, the mail server). The Application layer transfers the request to the Presentation layer.

The Presentation layer first determines whether and how it should format or encrypt the data request received from the Application layer. After it has made that determination, it adds any translation or codes required to implement that formatting and then passes your request on to the Session layer.

The Session layer picks up your formatted request and assigns a data token to it. A **token** is a special control frame that indicates to the rest of the network that you have the right to transmit data. (Remember that the Session layer acts as the "traffic cop" for communications between nodes.) The Session layer then passes your data to the Transport layer.

At the Transport layer, your data and the control information it has accumulated thus far are broken down into manageable chunks of data and prepared to be packaged in frames at the Data Link layer. If the data is too large to fit in one frame, the Transport layer subdivides it into several smaller blocks and assigns sequence identifiers to each block. This layer then passes the data blocks, one at a time, to the Network layer.

The Network layer adds addressing information to the data it receives from the Transport layer, so that subsequent layers will know the source and the destination of the data. It then passes the data blocks, with their addressing identifications, to the Data Link layer.

At the Data Link layer, the data blocks are packaged into individual frames. As you have learned, a frame is a structured format for transmitting small blocks of data. Using frames reduces the possibility of lost data or errors on the network, because each frame has its own built-in error check. This error checking algorithm, also known as the **Frame Check Sequence (FCS)**, is inserted at the end of the frame by the Data Link layer. In addition, the Data Link layer adds a header to the frame that incorporates destination and source addresses assigned by the Network layer. (Frame types and specifications are discussed in more detail in the next section.) The Data Link layer then passes the frames to the Physical layer.

Finally, your request for your mail message hits the NIC at the Physical layer. The Physical layer does not interpret the frame or add information to the frame; it simply delivers the data to the cabling and sends it across the network. Once the data arrives at the Physical layer of the remote system, the mail server's Data Link layer begins to unravel your request, reversing the process just described, until it responds to your request with its own transmission, beginning from its Application layer. Figure 2-3 shows how data is transferred from your system to the server, then back to your system through the OSI Model.

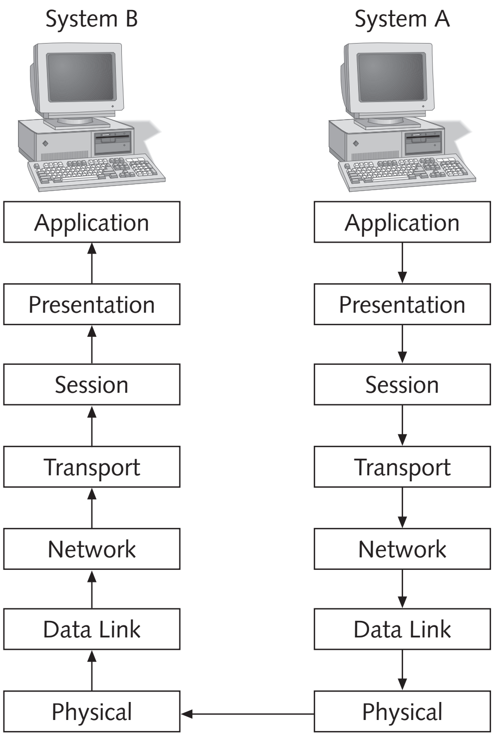

Figure 2-3 Data transfer between two systems

In the preceding example, you learned that every successive layer in the OSI Model—beginning with the Application layer and ending with the Physical layer—adds some control, formatting, or addressing information to the data it handles. The receiving system then interprets and uses the added information as it reverses the process, passing data from the Physical layer back up to the Application layer. Between your initial software request and the network cable, your blocks of data grow larger as they accumulate more handling information. Figure 2-4 depicts the transformation of data as it travels through the OSI Model layers.

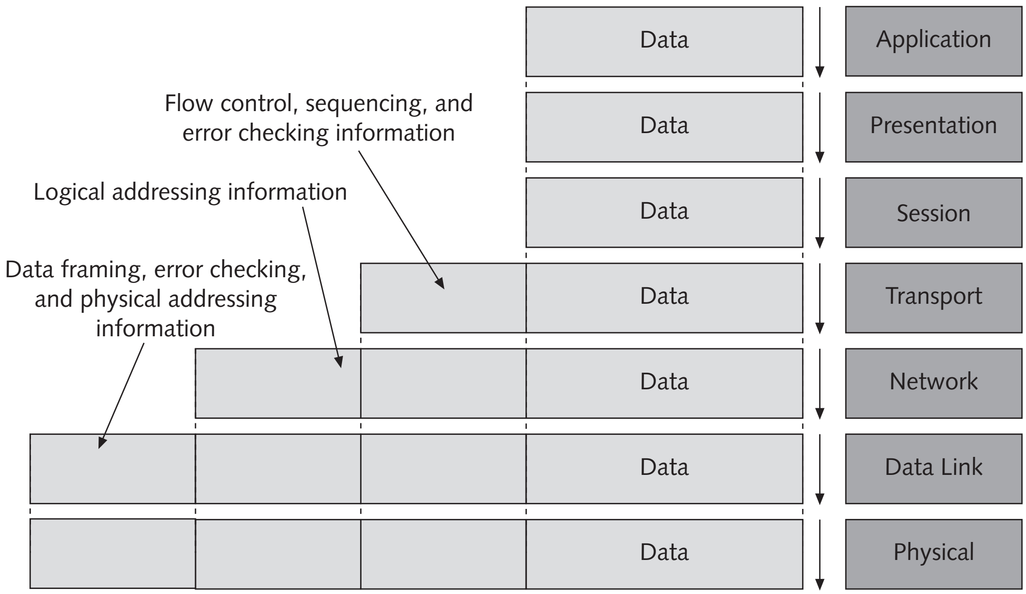

Figure 2-4 Data transformed through the OSI Model

Frame Specifications

Figure 2-2 introduced the basic structure of a data frame. In reality, frames are composed of several smaller components, or fields. The characteristics of these components depend on the type of network on which the frames run and on the standards that they must follow. The two major categories of frame types, Ethernet and Token Ring, correspond to the two most commonly used network technologies.

Ethernet is a networking technology originally developed at Xerox in the early 1970s and improved by Digital Equipment Corporation, Intel, and Xerox. Today, four types of Ethernet technology are used on LANs, with each type being governed by a set of IEEE standards. Ethernet LANs can transmit data at different rates and on a multitude of networking media. Ethernet is covered in detail in Chapter 5.

Token Ring is a networking technology developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology, passing around tokens that allow nodes to transmit data. Token Ring technology will be discussed in detail in Chapter 5.

Caution

Each frame type is unique and will not interact with different frame types on the network, because routers cannot support more than one frame type per physical interface. You can, however, work with multiple protocols on a network while using only one frame type. For example, you can run both IPX/SPX and TCP/IP on an Ethernet network. Although you can conceivably transmit both Token Ring and Ethernet frames on a network, Ethernet interfaces cannot interpret Token Ring frames, and vice versa. Normally, LANs use *either* Ethernet or Token Ring. On the other hand, many LANs run both TCP/IP *and* IPX/SPX.

It's important to know what frame type (or types) your network environment requires. You will use this information when installing network operating systems, configuring servers and client workstations, installing NICs, troubleshooting network problems and purchasing network equipment. It's also important to know what constitutes the frame. The following sections describe two typical frame types, Ethernet 802.3 and Token Ring 802.5.

A Typical Ethernet Frame

Figure 2-5 depicts a typical Ethernet frame as specified by the IEEE **802.3** standard.

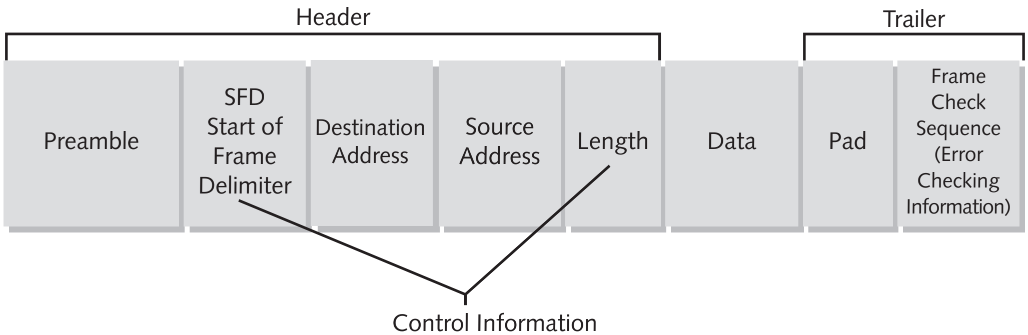

Figure 2-5 Ethernet frame as specified by the IEEE 802.3 standard

The components of the Ethernet 802.3 frame are described in the following list:

- *Preamble*—Marks the beginning of the entire frame, providing a signal that essentially announces to the network that data is en route. Because this field is part of the communications process, a preamble typically isn't included when calculating the size of a frame.
- *Start of Frame Delimiter (SFD)*—Indicates the beginning of the addressing frame.
- *Destination Address*—Contains the destination node address.
- *Source Address*—Contains the address of the originating node.
- *Length (LEN)*—Indicates the length of the packet.
- *Data*—Contains the data, or segmented part of that data, transmitted from the originating node.
- *Pad*—Used to increase the size of the frame to its minimum size requirement of 46 bytes.
- *Frame Check Sequence (FCS)*—Provides an algorithm to determine whether the data were received correctly. The most commonly used algorithm is called **Cyclic Redundancy Check (CRC)**, so you may also see this field called "CRC."

Chapter 5 provides more detail on this type of Ethernet frame. Chapter 5 also covers the other three Ethernet frame types.

A Typical Token Ring Frame

Figure 2-6 depicts a typical Token Ring frame, which is specified in the IEEE **802.5** standard. Note that some of its characteristics match those of the Ethernet frame, but significant differences arise in how the control information is handled.

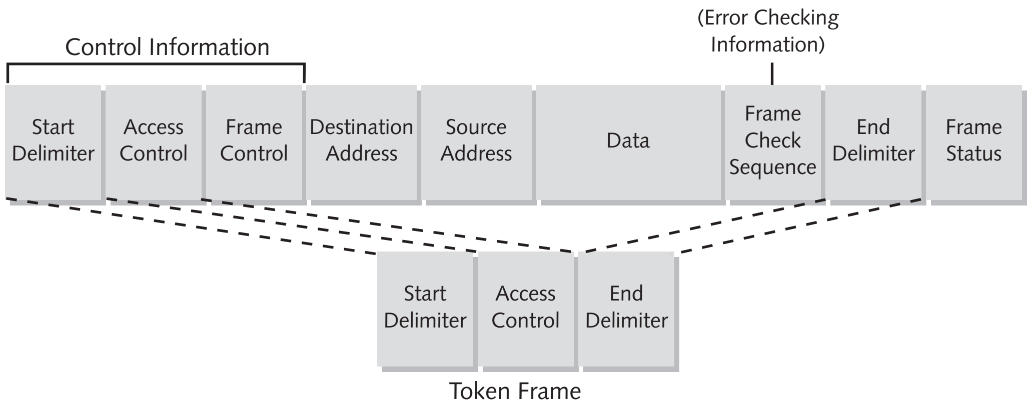

Figure 2-6 A typical Token Ring frame

The following list describes the components of the typical Token Ring frame:

- *Start Delimiter (SD)*—Signifies the beginning of the packet. It is one of three fields that compose the Token Ring frame.
- *Access Control (AC)*—Contains information about the priority of the frame. It is the second of three fields that compose the Token Ring frame.
- *Frame Control (FC)*—Defines the type of frame; used in the Frame Check Sequence.
- *Destination Address*—Contains the destination node address.
- *Source Address*—Contains the address of the originating node.
- *Data*—Contains the data transmitted from the originating node. May also contain routing and management information.
- *Frame Check Sequence (FCS)*—Used to check the integrity of the frame.
- *End Delimiter (ED)*—Indicates the end of the frame. It is the third field that composes the Token Ring frame.
- *Frame Status (FS)*—Indicates whether the destination node recognized and correctly copied the frame, or whether the destination node was not available.

Token Ring networks and frame types will be covered in more detail in Chapter 5.

Addressing Through the Layers

In Chapter 1, you learned that addressing is a system for assigning unique identification numbers to each node on a network. In this chapter, you learned that addressing is interpreted at the network layer of the OSI Model. In fact, each node on a network can be identified by two types of addresses: Network layer addresses and Data Link layer addresses.

Data Link layer addresses are fixed numbers associated with the networking hardware; they are usually assigned at the factory. These addresses are also called **MAC addresses**, after the **Media Access Control (MAC) sublayer**, which lies within the Data Link layer and appends the physical address of the destination to the data frame. MAC addresses are guaranteed to be unique because industry standards (established and maintained by IEEE) specify which numbers each manufacturer can use. For example, Ethernet NICs manufactured by the 3Com Corporation begin with the six-character sequence "00608C," while Ethernet NICs manufactured by Intel begin with "00AA00." The part of the MAC address that is unique to a particular vendor is called the **Block ID**. Some manufacturers have several different Block IDs. The remaining six characters in the sequence are added at the factory, based on the NIC's model and manufacture date, and collectively form the **Device ID**. An example of a Device ID assigned by a manufacturer might be 005499. The combination of the Block ID and Device ID result in a unique, 12-digit MAC address of 00608C005499. Networks rely upon unique MAC addressing to transmit data to their correct destination.

Note

Data Link layer—or MAC—addresses are also called physical addresses or hardware addresses.

Network layer addresses, which reside at the network level of the OSI Model, follow a hierarchical addressing scheme and can be assigned through operating system software. They are hierarchical because they contain subsets of data that incrementally narrow down the location of a node, just as your home address is hierarchical because it provides a country, state, zip code, city, street, house number, and person's name. Network Layer addresses, therefore, are more useful to internetworking devices such as routers, because they make sorting data more logical. Network layer address formats differ depending on which protocols the network uses. Chapter 3 covers the addressing rules for the different protocols.

Note

Network layer addresses are also called logical addresses or virtual addresses.

IEEE Networking Specifications

In addition to frame types, the IEEE networking specifications apply to connectivity, networking media, error checking algorithms, encryption, emerging technologies, and more. All of these specifications fall under the IEEE's "Project 802," an effort to standardize physical elements of a network. IEEE developed these standards before the OSI Model was standardized by ISO, but IEEE's 802 standards can be applied to the layers of the OSI Model. Table 2-2 describes the IEEE 802 specifications. You should be familiar with the topics that each standard covers. The Network+ certification exam includes questions about IEEE 802 specifications.

Table 2-2 IEEE 802 standards

Standard	Name	Explanation
802.1	Internetworking	Covers routing, bridging, and internetwork communications
802.2	Logical Link Control	Relates to error and flow control over data frames
802.3	Ethernet LAN	Covers all forms of Ethernet media and interfaces
802.4	Token Bus LAN	Covers all forms of Token Bus media and interfaces
802.5	Token Ring LAN	Covers all forms of Token Ring media and interfaces
802.6	Metropolitan Area Network (MAN)	Covers MAN technologies, addressing, and services
802.7	Broadband Technical Advisory Group	Covers broadband networking media, interfaces, and other equipment
802.8	Fiber-Optic Technical Advisory Group	Covers use of fiber-optic media and technologies for various networking types
802.9	Integrated Voice/Data Networks	Covers integration of voice and data traffic over a single network medium
802.10	Network Security	Covers network access controls, encryption, certification, and other security topics
802.11	Wireless Networks	Standards for wireless networking for many different broadcast frequencies and usage techniques
802.12	High-Speed Networking	Covers a variety of 100Mbps-plus technologies, including 100BASEVG-AnyLAN

To accommodate shared access for multiple network nodes (as opposed to simple point-to-point communication), the IEEE expanded the OSI Model by separating the Data Link layer into two sublayers: the Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer. The **LLC**, the upper sublayer in the Data Link layer, provides a common interface and supplies reliability and flow control services. The **MAC**, the lower sublayer of the Data Link layer, actually appends the physical address of the destination computer onto the data frame. IEEE's specifications for Ethernet and

Token Ring technology (found in Table 2-2) apply to the MAC sublayer of the Data Link layer. Figure 2-7 shows how the IEEE subdivided the Data Link layer.

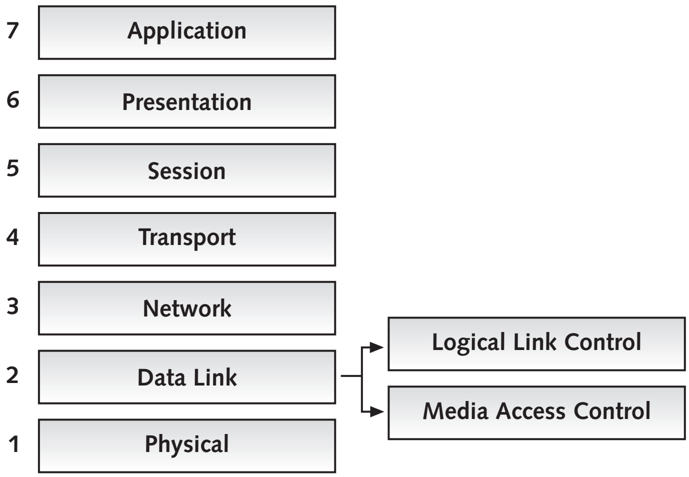

Figure 2-7 The Logical Link Control and Media Access Control sublayers

CHAPTER SUMMARY

- Standards are documented agreements containing technical specifications or other precise criteria that are used as guidelines to ensure that materials, products, processes, and services suit their purpose. Without standards, you could not design a network because your hardware would not fit together and your programs could not communicate with each other.
- A complete compilation of standards that apply to the networking and computer industries would fill an encyclopedia. Some of the significant standards organizations are ANSI (American National Standards Institute), EIA (Electronic Industries Alliance), IEEE (Institute of Electrical and Electronic Engineers), ISO (International Organization for Standardization), and ITU (International Telecommunications Union, formerly called the CCITT).
- In the early 1980s, ISO began work on a universal set of specifications that would enable computer platforms across the world to communicate openly. The result was a helpful model for understanding and developing computer-to-computer communication. This model, called the Open Systems Interconnection (OSI) Model, divides networking architecture into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application. Each layer has its own set of functions and interacts with the layers directly above and below it.
- The Physical layer is the lowest, or first, layer of the OSI Model. It contains the physical networking medium, such as cabling, connectors, and repeaters. Protocols

at the Physical layer generate and detect voltage so as to transmit and receive signals carrying data. The Physical layer sets the data transmission rate and monitors data error rates, though it does not provide error correction.

- The second layer of the OSI Model, the Data Link layer, bridges the networking media with the abstract software and data streams. Its primary function is to divide data it receives from the Network layer into frames that can then be transmitted by the Physical layer. Connectivity devices such as bridges and switches work in the Data Link layer, because they decode frames and use the frame information to transmit data to its correct recipient.

- The Network layer, the third OSI Model layer, manages addressing and routing data based on addressing, patterns of usage, and availability. Routers belong to the Network layer because they use this information to intelligently direct data from sender to receiver. The Network layer is also responsible for segmentation and reassembly of packets.

- The Transport layer is primarily responsible for ensuring that data are transferred from point A to point B (which may or may not be on the same network segment) reliably and without errors. For example, the Transport layer ensures that data are sent and received in the same order, or sequence. It also establishes the level of packet error checking.

- The Session layer establishes and maintains communication between two nodes on the network. It can be considered the "traffic cop" of network communications. The term "session" refers to a connection for data exchange between two parties; it is most often used in the context of terminal and mainframe communications.

- The Presentation layer, the sixth OSI Model layer, serves as a translator between the application and the network. At the Presentation layer, data are formatted in a schema that the network can understand; this format varies with the type of network used. The Presentation layer also manages data encryption and decryption, such as the scrambling of system passwords.

- The top, or seventh, layer of the OSI Model is the Application layer. It provides interfaces to the software that enable it to use network services. Some of the services provided by the Application layer include file transfer, file management, and message handling for electronic mail.

- A data request from a software program is received by the Application layer services and is transferred down through the layers of the OSI Model until it reaches the Physical layer, or the network cable. At that point, data are sent to their destination over the wire, and the Physical layer services at the destination send it back up through the layers of the OSI Model until it reaches the Application layer.

- Data frames, also known simply as "frames," are small blocks of data with control, addressing, and handling information attached to them. Frames are composed of several smaller components. The characteristics of these components depend on the type of network on which the frames run and the standards that they must follow. The two

major categories of frame types, Ethernet and Token Ring, correspond to the two most commonly used network technologies.

- Each node on a network can be identified by two types of addresses: Network layer addresses and Data Link layer addresses. Data Link layer addresses are hardwired into the networking device, and are also called physical, MAC, or hardware addresses. Network layer addresses, also called logical or virtual addresses, are assigned to devices through operating software. These logical addresses are composed of hierarchical information, so they can be easily interpreted by routers and used to direct data to their destinations.
- In addition to frame types, the IEEE networking specifications apply to connectivity, networking media, error checking algorithms, encryption, emerging technologies, and more. All of these specifications fall under the IEEE's Project 802, an effort to standardize the elements of networking.
- The IEEE expanded the OSI Model by separating the Data Link layer into two sublayers: the Logical Link Control (LLC) sublayer and the Medium Access Control (MAC) sublayer. The LLC, the upper sublayer in the Data Link layer, provides a common interface and supplies reliability and flow control services. The MAC, the lower sublayer of the Data Link layer, actually appends the physical address of the destination computer onto the data frame.

KEY TERMS

802.3 — The IEEE standard for Ethernet networking devices and data handling.

802.4 — The IEEE standard for Token Bus networking devices and data handling.

802.5 — The IEEE standard for Token Ring networking devices and data handling.

802.6 — The IEEE standard for Metropolitan Area Network (MAN) networking.

802.10 — The IEEE standard that describes network access controls, encryption, certification, and other security topics.

802.11 — The IEEE standard for wireless networking.

acknowledgment (ACK) — A response generated at the Transport layer of the OSI Model that confirms to a sender that its frame was received.

ANSI (American National Standards Institute) — An organization composed of more than 1000 representatives from industry and government who together determine standards for the electronics industry in addition to other fields, such as chemical and nuclear engineering, health and safety, and construction.

Application layer — The seventh layer of the OSI Model. The Application layer provides interfaces to the software that enable programs to use network services.

application programming interface (API) — A routine (or set of instructions) that allows a program to interact with the operating system. APIs belong to the Application layer of the OSI Model.

Block ID — The first set of six characters that make up the MAC address and that are unique to a particular vendor.

Cyclic Redundancy Check (CRC) — An algorithm used to verify the accuracy of data contained in a data frame.

Data Link layer — The second layer in the OSI Model. The Data Link layer bridges the networking media with the Network layer. Its primary function is to divide the data it receives from the Network layer into frames that can then be transmitted by the Physical layer.

Data Link layer address — See *MAC address*.

Device ID — The second set of six characters that make up a network device's MAC address. The Device ID, which is added at the factory, is based on the device's model and manufacture date.

EIA (Electronic Industries Alliance) — A trade organization composed of representatives from electronics manufacturing firms across the United States.

Ethernet — A networking technology originally developed at Xerox in 1970 and improved by Digital Equipment Corporation, Intel, and Xerox. Today, four types of Ethernet technology are used on LANs, with each type being governed by a set of IEEE standards.

flow control — A method of gauging the appropriate rate of data transmission based on how fast the recipient can accept data.

frame — A package for data that includes not only the raw data, or "payload," but also the sender's and receiver's network addresses and control information.

Frame Check Sequence (FCS) — The field in a frame responsible for ensuring that data carried by the frame arrives intact. It uses an algorithm, such as CRC, to accomplish this verification.

IEEE (Institute of Electrical and Electronic Engineers) — An international society composed of engineering professionals. Its goals are to promote development and education in the electrical engineering and computer science fields.

ISO (International Organization for Standardization) — A collection of standards organizations representing 130 countries with headquarters located in Geneva, Switzerland. Its goal is to establish international technological standards to facilitate the global exchange of information and barrier-free trade.

ITU (International Telecommunication Union) — A United Nations agency that regulates international telecommunications, including radio and TV frequencies, satellite and telephony specifications, networking infrastructure, and tariffs applied to global communication. It also provides developing countries with technical expertise and equipment to advance these nations' technological bases.

logical address — See *Network layer addresses*.

Logical Link Control (LLC) sublayer — The upper sublayer in the Data Link layer. The LLC provides a common interface and supplies reliability and flow control services.

MAC address — A number that uniquely identifies a network node. The manufacturer hard-codes the MAC address on the NIC. This address is composed of the Block ID and Device ID.

Media Access Control (MAC) sublayer — The lower sublayer of the Data Link layer. The MAC appends the physical address of the destination computer onto the frame.

Microsoft Message Queueing (MSMQ) — An API used in a network environment. MSMQ stores messages sent between nodes in queues then forwards them to their destination based on when the link to the recipient is available.

network address — See *Network layer addresses*.

network architect — A professional who designs networks, performing tasks that range from choosing basic components (such as cabling type) to figuring out how to make those components work together (by, for example, choosing the correct protocols).

Network layer — The third layer in the OSI Model. The Network layer translates network addresses into their physical counterparts and decides how to route data from the sender to the receiver.

Network layer addresses — Addresses that reside at the Network level of the OSI Model, follow a hierarchical addressing scheme, and can be assigned through operating system software.

Open Systems Interconnection (OSI) Model — A model for understanding and developing computer-to-computer communication developed in the 1980s by ISO. It divides networking architecture into seven layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

physical address — See *MAC address*.

Physical layer — The lowest, or first, layer of the OSI Model. The Physical layer contains the physical networking media, such as cabling and connectors.

Presentation layer — The sixth layer of the OSI Model. The Presentation layer serves as a translator between the application and the network. Here data are formatted in a schema that the network can understand, with the format varying according to the type of network used. The Presentation layer also manages data encryption and decryption, such as the scrambling of system passwords.

reassembly — The process of reconstructing data units that have been segmented.

route — To direct data between networks based on addressing, patterns of usage, and availability of network segments.

routers — Devices that connect network segments and intelligently direct data based on information contained in the data frame.

segmentation — The process of decreasing the size of data units when moving data from a network segment that can handle larger data units to a network segment that can handle only smaller data units.

sequencing — The process of assigning a placeholder to each piece of a data block to allow the receiving node's Transport layer to reassemble the data in the correct order.

session — A connection for data exchange between two parties. The term "session" is most often used in the context of terminal and mainframe communications.

Session layer — The fifth layer in the OSI Model. The Session layer establishes and maintains communication between two nodes on the network. It can be considered the "traffic cop" for network communications.

standards — Documented agreements containing technical specifications or other precise criteria that are used as guidelines to ensure that materials, products, processes, and services suit their intended purpose.

terminal — A device with little (if any) of its own processing or disk capacity that depends on a host to supply it with applications and data-processing services.

token — A special control frame that indicates to the rest of the network that a particular node has the right to transmit data.

Token Ring — A networking technology developed by IBM in the 1980s. It relies upon direct links between nodes and a ring topology, using tokens to allow nodes to transmit data.

Transport layer — The fourth layer of the OSI Model. The Transport layer is primarily responsible for ensuring that data are transferred from point A to point B (which may or may not be on the same network segment) reliably and without errors.

Review Questions

1. Which international standards organization is part of the United Nations?
   a. IEEE
   b. ITU
   c. ISO
   d. ANSI
2. What does "ISO" stand for?
   a. Institute for Standards Organization
   b. International Standards Organization
   c. International Organization for Standardization
   d. International Statisticians Organization
3. Which organization represents the United States in ISO?
   a. ANSI
   b. ITU
   c. IEEE
   d. EIA

4. Which technology is standardized in the IEEE 802.5 specification?
   a. network security
   b. Token Ring LANs
   c. wireless networks
   d. Ethernet LANs
5. Which technology is standardized in the IEEE 802.3 specification?
   a. network security
   b. Token Ring LANs
   c. wireless networks
   d. Ethernet LANs
6. Which layer of the OSI Model provides file transfer services?
   a. Application layer
   b. Data Link layer
   c. Transport layer
   d. Presentation layer
7. Netscape is an example of a program that runs in the Application layer. True or False?
8. Which layer of the OSI Model establishes the rules of communication between two nodes?
   a. Transport layer
   b. Session layer
   c. Data Link layer
   d. Presentation layer
9. In which layer of the OSI Model do switches and bridges belong?
   a. Data Link layer
   b. Transport layer
   c. Network layer
   d. Session layer
10. In which layer of the OSI Model do routers belong?
   a. Data Link layer
   b. Transport layer
   c. Network layer
   d. Physical layer

11. In which two layers of the OSI Model do NICs belong?
    a. Presentation and Application layer
    b. Transport and Network layer
    c. Network and Data Link layer
    d. Physical and Data Link layer
12. Which standards organization developed the OSI Model?
    a. IEEE
    b. ITU
    c. OSI
    d. ISO
13. Under what circumstances would the Network layer use segmentation?
    a. when too many data frames are flooding into a receiving node's NIC
    b. when the network is transmitting too many incorrect frames
    c. when the destination node cannot accept the size of the data blocks transmitted by the source node
    d. when the source node requests that data blocks be segmented for faster processing
14. Generating and detecting voltage so as to transmit and receive signals carrying data is the responsibility of which OSI Model layer?
    a. Transport layer
    b. Session layer
    c. Presentation layer
    d. Physical layer
15. Flow control is the process of making sure data frames are received in the correct order. True or False?
16. What is the purpose of a token in a token-passing network?
    a. It indicates to the rest of the network that one node has the right to transmit data.
    b. It indicates to the rest of the network that one node is busy and cannot receive traffic.
    c. It indicates to the rest of the network that a broadcast message is about to be sent.
    d. It indicates to the rest of the network that one node is causing transmission errors for the rest of the network.

17. If you use a password to log in to your Microsoft Exchange program, which layer of the OSI Model would decode your password?
    a. Application layer
    b. Session layer
    c. Presentation layer
    d. Network layer
18. Which layer of the OSI Model handles error checking and retransmission of bad data?
    a. Transport layer
    b. Network layer
    c. Session layer
    d. Physical layer
19. What are the differences between MAC addresses and Network layer addresses?
20. One frame type will not interact with another frame type on the network. True or False?
21. Which of the following types of addresses follow a hierarchical format?
    a. Physical layer addresses
    b. MAC addresses
    c. Network layer addresses
    d. Data Link layer addresses
22. Which of the following is not a field found in an Ethernet 802.3 data frame?
    a. path selector
    b. destination address
    c. source address
    d. length
23. Token Ring technology was originally developed by which company?
    a. Hewlett-Packard
    b. IBM
    c. Cisco
    d. 3Com
24. Which of the following is not a field found in a Token Ring data frame?
    a. frame status
    b. source address
    c. destination address
    d. pad

25. A single frame type can support only one kind of protocol. True or False?
26. What are the sublayers of the Data Link layer as defined in the IEEE 802 standards?
    a. Logical Link Control sublayer and Media Access Control sublayer
    b. Transport Control sublayer and Media Access Control sublayer
    c. Logical Link Control sublayer and Physical Addressing sublayer
    d. Transport Control sublayer and Data Link Control sublayer
27. Describe the functions of the two Data Link layer sublayers.
28. What is the purpose of a router?
29. What part of the MAC address is unique to each vendor?
    a. the destination ID
    b. the Block ID
    c. the physical node ID
    d. the segment ID
30. IEEE has standardized four Ethernet frame types. True or False?

HANDS-ON PROJECTS

Project 2-1

To better understand the impact IEEE has on networking standards, it is helpful to look at some of the specifications developed by IEEE. This exercise will guide you through the process of searching for IEEE specifications on the Web. To complete this project, you need a computer with access to the Internet.

1. Access the Internet and go to www.standards.ieee.org.
2. On the Standards page, click the **IEEE Standards Online** link.
3. Under the heading "IEEE Standards Online Subscriptions," click the **SEARCH** link.
4. The IEEE Standards Online Search Web page appears.
5. Beneath the search text box, click **Advanced** to access advanced search options.
6. Type **Ethernet** in the text box below the first search parameter line.
7. Leave the other options on the search page as they are, then click **seek** to execute your search.
8. Note how many abstracts your search returned. For those abstracts that give designation numbers, note the numbers as well.
9. What was the date of the last 802.3 CSMA/CD standards revision? Why do you suppose this standard would be updated so frequently?

Project 2-2

When supporting computers on a network, you will often need to change the network properties on client workstations. You may perform this task when you first set up a machine or later, if it is having problems or if the network specifications have changed. This exercise introduces you to the process of finding and changing network properties on a client workstation. You will need to be familiar with this process not only to be a successful networking professional, but also to qualify for Net+ certification.

This project requires a desktop computer client running Windows 2000 Professional and both the TCP/IP and IPX/SPX protocols connected to a Windows 2000 server running on an Ethernet network. (You will learn more about the TCP/IP and IPX/SPX protocols in Chapter 3.)

1. On the Windows 2000 Professional computer, click **Start**, point to **Settings**, then click **Network and Dial-up Connections**. The Network and Dial-up Connections window opens.
2. Right-click **Local Area Connection** and then click **Properties** in the shortcut menu. The Local Area Connection Properties dialog box appears.
3. Scroll down the list of installed components until you find the NWLink IPX/SPX/NetBIOS-Compatible Transport Protocol, then double-click this service to see its properties.
4. Note your workstation's current Ethernet frame type. Click the down arrow next to the frame type setting to view other frame type options.
5. Change the frame type value to **Ethernet SNAP**, then click OK to save your change.
6. Click **OK** again to close the Local Area Connection Properties dialog box.
7. To make sure the changes have taken effect, reboot your computer.
8. Note what happens after you restart your computer and try to connect to the network. Do you have trouble making a connection, or does the network accept your login ID and password? Why or why not?
9. To ensure that your workstation will function properly on the network once again, you should restore your original frame type settings. To do so, repeat Steps 1 through 4. In the Frame type properties list, select the original frame type you noted in Step 5.
10. Click **OK** to save your change, then click **OK** to continue.
11. To make sure the changes have taken effect, reboot your computer.

Project 2-3

You will need to know how to find and interpret MAC addresses when supporting networks. In this exercise, you will discover two ways of finding your computer's MAC address, also known as its physical address, or sometimes, its adapter address. For this exercise you will need a workstation running the Windows 2000 Professional operating system

and the TCP/IP protocols connected to a Windows 2000 server. You will also need a screwdriver that fits the workstation's cover screws, if the computer's cover is attached with screws.

1. On the Windows 2000 Professional computer, click **Start**, point to **Programs**, point to **Accessories**, and then click **Command Prompt**. The Command Prompt window opens with a cursor blinking at the C:\> prompt.
2. Type **ipconfig/all** then press **Enter**. A list of your Windows 2000 IP Configuration and Ethernet adapter Local Area Connection parameters appears. This includes your workstation's TCP/IP properties, as well as its MAC address.
3. Search the list for the Physical Address parameter. This 12-digit hexadecimal number is your NIC's MAC address.
4. Type **exit** and press Enter to close the Command Prompt window.
5. Log off the network and shut down your workstation.
6. If necessary, use the screwdriver to remove the screws that secure the workstation's housing. Ask your instructor for help if you can't find the correct screws. Usually there are three to five screws. In some cases, a computer housing may use no screws.
7. Remove the cover from the rest of the CPU.
8. If a cable is connected to your NIC, remove the cable.
9. With the computer open, remove the screw that holds the NIC in place. Gently remove the NIC from its place in the computer's motherboard.
10. In most cases, a NIC's MAC address is printed on a small white sticker attached to the NIC; alternatively, it may be stamped directly on the NIC itself. Find the MAC address and compare it to the one you discovered in Step 3.
11. Reinsert the NIC into its slot so that it is secure and replace the screw that holds it in.
12. Replace the computer's cover and the screws that fasten it to the CPU.

CASE PROJECTS

Case Project

1. You are a networking professional who works in a college computer lab. The computers run only the TCP/IP protocol on an Ethernet network, and all computers use 3Com NICs. Many beginning computer science students use this lab for homework; you help them access the network and troubleshoot problems with their connections on a daily basis. One day a student begins tampering with his computer; when he restarts the computer, it alerts him that it can't find the network. In a step-by-step fashion, explain the approach you take to find and fix the problem.

   (Your drive letter may vary, depending on how you installed Windows 2000 Professional.)

2. The same student is curious about how a Web site appears on his computer screen. On a separate piece of paper, draw and explain the process that occurs between a client and a server when requesting a Web page, using the OSI Model as a reference. Explain to the student why each step is important and how it contributes to data arriving in the correct place without errors.
3. The student appreciates the time you spent explaining what happens to the data as it moves through the OSI Model layers, but he wonders why he should ever care about the OSI Model or data frames. He says he wants to become a network architect and concern himself with routers, switches, and cabling. The student indicates that he doesn't care about the little details like packets. In response, draw a picture of an Ethernet data frame and identify its fields. Describe how these fields can affect a network's design and networking in general.